Information Security Failures Measured and ISO/IEC 27001:2022 Controls Ranked by General Data Protection Regulation Penalty Analysis

Information Security Failures Measured and ISO/IEC 27001:2022 Controls Ranked by General Data Protection Regulation Penalty Analysis

Mikko Suorsa
School of Technology and Innovations
University of Vaasa
Vaasa, Finland
ORCiD: 0000-0002-1649-4223

Petri Helo
School of Technology and Innovations
University of Vaasa
Vaasa, Finland
ORCiD: 0000-0002-0501-2727

***Abstract*—Selecting the most important information security controls is a critical and difficult process. Therefore, the decision-making on how to manage risks and threats has to be supported with data-driven performance measurement metrics. This paper identifies and explores the failures and impacts of information security, as well as the most effective controls to mitigate information security risks in organizations. The method of the study was root cause analysis. All year 2020 GDPR penalty cases (n=81) based on misconduct, as defined in GDPR Article 32: "Security of processing" were matched with ISO/IEC 27001:2022 controls, which were used as failure identifiers in the analysis. As a result, the study presents both, the top 10 most frequent and the top 10 most expensive information security failures corresponding to ISO/IEC 27001:2022 controls. Furthermore, the study also illustrates the correlation of these controls.**

Keywords— Information security, IT risk management, IT compliance, ISO/IEC 27001:2022, General Data Protection Regulation, GDPR

I. INTRODUCTION

Information is a very important asset of any organization and therefore failures in information security may not only threaten the success of organizations but also their continuation [1]. However, the identification, ranking, and decision to apply the most crucial information security controls to mitigate the risks and threats is a difficult process and a major management challenge [2].

Regulatory requirements to comply with information security and privacy laws are becoming more demanding [1]. The EU General Data Protection Regulation (GDPR) protects the privacy of EU citizens and requires all organizations operating within the EU to have sufficient control of information security [3]. Breaching the rules of GDPR can lead to large monetary sanctions, and enforcement actions have already been commenced [4].

Intelligence on information security failures and controls to effectively manage these failures is becoming an ever more important process in order to govern information security and compliance with regulations [5]. Therefore, optimized decisions when selecting the most impactful security controls should be based on data-driven performance measurement metrics [6].

International standardization frameworks play a decisive role in governing, assuring, and certifying effective information security in organizations [7], whereas the ISO 27001 is one of the most applied standards for determining the organization's information security controls [8]. However, studies ranking the most important ISO 27001 controls based on their effectiveness are limited.

Responses need to be undertaken on security controls to sufficiently meet the data protection requirements [9]; thus, research efforts are necessary to reduce the gap between regulation and information security [10]. GDPR penalties have already been studied and explored, but no studies have so far been conducted to specifically analyze GDPR penalty cases using statistical methods to identify information security failures with certification frameworks such as the controls in the ISO/IEC 27001:2022.

This leads us to the research problem of this paper, which is to identify and explore the failures and impacts of information security, as well as the most effective controls to mitigate information security risks in organizations. We address this problem with the research question: ***What are the most frequent and most expensive information security failures corresponding to ISO/IEC 27001:2022 controls, and what is their correlation?***

In this paper, we measure information security failures by performing a root cause analysis on European Union GDPR penalty case documents. All year 2020 penalties (n=81) throughout the EU member countries based on the definition of misconduct in GDPR Article 32, "Security of processing", were analyzed and matched with the ISO/IEC 27001:2013 standard controls, and after the new version ISO/IEC 27001:2022 was published, the results were migrated to correspond with the new version of the standard.

II. BACKGROUND

A. The EU General Data Protection Regulation

The EU GDPR came into force in May 2018, and the primary objective of the law is to protect the fundamental right of EU citizens to data protection and the processing of their personal data. GDPR brings forth a significant requirement for information security. The GDPR Article 32, "Security of processing", forces organizations to apply technical and organizational measures to ensure the adequate security of personal data [3].

The supervisory authorities acting in each EU member country have the task of ensuring compliance with the GDPR, and in order to fulfil this operation they have various investigative and corrective powers. The most stringent form of corrective power is administrative fines, where the maximum penalty is up to 20 million euros, or 4 % of the total global annual turnover of an organization [3].

GDPR sanctions are issued depending on certain criteria such as the nature, gravity, and duration of the infringement, which furthermore becomes public information, and therefore GDPR enables transparency in cases of data breaches caused by information security failures throughout the European Union member countries [11]. GDPR has allowed each EU

member state to enact its own rules on judging whether and to what extent penalties may be enforced on public organizations [3]. However, the European Data Protection Board, which ensures the consistent application of GDPR, has published guidelines to harmonize the different methodologies of the various national supervisory authorities.

Infringements which led to GDPR sanctions have already been explored and studied. One study analyzed GDPR penalty case documents with data mining techniques for the purpose of providing information about the penalty impacts of individual articles of GDPR [4]. GDPR penalty case documents have also been analyzed to provide intelligence about GDPR violation types and penalty amount categorizations [12] [13].

GDPR penalty case document analyses have also been supplemented with interviews to provide information about GDPR compliance risk identification and its respective mitigation [14]. However, no studies have so far been performed to specifically analyze GDPR penalty cases using statistical methods to identify information security failures with certification frameworks such as the controls in the new ISO/IEC 27001:2022.

B. *The ISO/IEC 27001:2022 in the ISO 27000 family of standards*

The ISO/IEC 27000 family of standards is a numbered series of international information security standards. The foundation of the ISO 27001:2022 standard requires organizations to apply an information security management system (ISMS) in order to implement a risk-based approach and administer controls to protect the confidentiality, integrity, and availability of information from threats and vulnerabilities. The ISO 27001:2022 controls are located in Annex A [15].

The sequential ISO/IEC 27002:2022 standard provides the guidelines for the implementation of an effective ISMS and controls in ISO 27001 Annex A [16]. ISO/IEC 27701:2019 is an auxiliary standard for both ISO 27001 and ISO 27002, and it defines requirements and further guidance for establishing a privacy information management system. It broadens the information security requirements of ISO 27001 to take into its scope the protection of privacy and personally identifiable information (PII) and provides direction on how these requirements should be implemented [17].

Studies show that the ISO 27001 framework has been used to construct information security risk assessment methodologies [18] and capability maturity model assessment tools for organizations [19]. One study categorized the ISO 27001 controls based on their effectiveness in supporting organizations in evaluating and enhancing their ISMS conduct, as well as providing an understanding of relevant security flaws [20].

Another study was conducted with fuzzy analytic hierarchy process to rank the ISO 27001 controls [21], while further studies analyzed the GDPR requirement with ISO 27001 controls to provide information about their synergies [9], and it was suggested that ISO 27001 is a GDPR compliance facilitator [22]. However, currently, there are no studies addressing information security failures with statistical methods based on the new ISO/IEC 27001:2022 controls and further ranking them.

III. MATERIAL AND METHOD

A. *Material search*

The publicly available data source for this study is the GDPR Enforcement Tracker, which is a freely accessible website maintained by a global law firm, CMS. The database accommodates reports on cases of formal GDPR penalties issued by the authorities in EU member countries to organizations not adhering to the law [23].

The database was searched through filtering by the year 2020, together with GDPR Article 32 “Security of processing”, which resulted in 81 GDPR penalty case reports, where the penalty type was “insufficient technical and organizational measures to ensure information security”. These GDPR penalty case reports, formally defining information security failures, accounted for the penalties issued to 81 different organizations.

B. *Method*

The method applied in the study was root cause analysis (RCA) to identify what caused the information security failures and what their impacts were. Root cause analysis as a method is a process which applies data collection, cause charting, root cause identification, and generation of recommendations. Only when root causes are determined can corrective measures that prevent future events of the type observed be specified [24].

The different RCA subtype methods can be summarized into the following three categories: a) chart type RCAs, which are constructed in the style of a flow chart, b) tabular type RCAs, which are constructed in a table with predefined column headings and categories and c) graphical RCAs, which visualize the results in a bar graph or any graphical display of numerical data [25]. The RCA method of this study is a mixture of tabular and graphical RCA types.

C. *Set of criteria and the analysis*

The criteria for this analysis were first the ISO/IEC 27001:2013 Annex A controls, which were initially used as root cause identifiers in each of 81 GDPR penalty cases [26]. Data was collected in a table which consisted of information about every GDPR penalty case and binary values corresponding to a specific information security failure, as exemplified in Table 1.

TABLE I. *GDPR PENALTY CASES AND INFORMATION SECURITY FAILURE BINARY VALUES*

	Penalty	**Failure a**	**Failure b**	**Failure c**
Case 1	10.000 €	0	1	1
Case 2	5000 €	1	1	1
Case 3	100.000 €	1	0	1
Case 4	8000 €	1	0	0
Case 5	600.000 €	1	0	0
Total	**723.000 €**	**4**	**2**	**3**

When this study was conducted, a new version of ISO/IEC 27001:2022 was published in Q4 2022 and the results were migrated to match the new version of the standard. As a result, 32 individual information security failures were identified, which included five failures that

could not be matched with any of ISO/IEC 27001:2022 controls.

These five failures were, however, included in the scope of the analysis because they were explicitly addressed by the supervisory authorities, and consequently were the cause of the issued penalties. In the presented results, these unmatched information security failures do not have the ISO number prefix, unlike the failures which were mapped to a specific ISO/IEC 27001:2022 control.

Penalty amount calculations for each information security failure were determined in the following way. The total penalty of a single GDPR penalty case was divided by the number of information security failures detected in the case. For example, in GDPR penalty case 1, illustrated in Table 1, with two detected information security failures and a total penalty of 10,000 euros, the cost of an individual failure was 5,000 euros. After that, the average was calculated for all information security failures, which became the penalty for each failure.

In the correlation analysis, p-values of the Pearson correlation were used, and outcomes where the p-value was lower than 0.05 were considered statistically significant. Information security failures which had a fairly strong (0.30 and above) correlation and statistical significance (p-value lower than 0.05), consisted of a total of 44 observations.

IV. Results

In this section, the results of the analysis are presented and discussed. ISO/IEC 27001:2022, ISO/IEC 27002:2022, and ISO/IEC 27701:2019 standards are used for interpreting the results.

A. The most frequent information security failures

The top 10 most frequent information security failures corresponding to ISO/IEC 27001:2022 controls are presented in Table 2.

TABLE II. *Top 10 most frequent information security failures corresponding to ISO/IEC 27001:2022 controls*

Control	Frequency	Penalty
8.3 Information access restriction	47	238,035 €
6.3 Information security awareness, education and training	32	40,604 €
5.12 Classification of information	31	623,332 €
5.14 Information transfer	18	10,182 €
8.24 Use of cryptography	18	335,304 €
8.15 Logging	14	331,892 €
8.29 Security testing in development and acceptance	14	1,146,388 €
5.10 Acceptable use of information and other associated assets	12	69,025 €
Human error	12	175,918 €
5.19 Information security in supplier relationships	9	343,139 €

The most common failure is the absence of "8.3 Information access restriction", where many cases showed that employees had unauthorized access to information that they should not have had. Another significant reason for data breaches is the insufficient "6.3 Information security awareness, education and training". Deficiencies in this control lead to a range of severe problems because employees are unaware of what is expected of them.

Another very critical failure is caused by insufficient implementation of "5.12 Classification of information", whereas information shall be classified based on organizational security needs and relevant interested party requirements, as well as PII [15] [17]. If this process is not carried out, relevant risk based controls cannot be applied, which leads to considerable compliance flaws [16].

The lack of control over "5.14 Information transfer" is a frequent failure. Unsecure and careless electronic messaging, including email, electronic data exchange, and social networking, often led to incidents. Another frequent failure is the unsuccessful implementation of "8.24 Use of cryptography". The type and strength of the cryptographic techniques required should be determined based on the classification of information [15].

A frequent failure is inadequate "8.15 Logging" because the lack of tracing user activities and access to PII in systems often led to data breaches. The absence of "8.29 Security testing in development and acceptance" was a cause of many failures. If proper security testing processes are not implemented during the system development life cycle, vulnerabilities are not discovered and fixed.

The lack of control over "5.10 Acceptable use of information and other associated assets" is a common cause of data breaches, followed by "Human error", which is not mapped to any specific ISO 27001 control. This failure, often resulting from insufficient information security awareness and training programs, can be further traced to poor organizational processes.

Finally, the absence of control over "5.19 Information security in supplier relationships", which is also a direct GDPR requirement [3], is a frequent cause among data breaches, underscoring the need for risk management related to the use of suppliers' products or services [15].

B. The most expensive information security failures

The top 10 most expensive information security failures corresponding to ISO/IEC 27001:2022 controls are presented in Table 3.

TABLE III. *Top 10 most expensive information security failures corresponding to ISO/IEC 27001:2022 controls*

Control	Penalty	Frequency
Technical data quality inconsistencies in systems leading to confidentiality breach	9,266,667 €	1
8.2 Privileged access rights	2,138,202 €	2
8.7 Protection against malware	1,214,167 €	2
8.29 Security testing in development and acceptance	1,146,388 €	14
8.32 Change management	765,217 €	3
5.12 Classification of information	623,332 €	31
5.24 Information security incident management planning and preparation	518,694 €	4
8.31 Separation of development, test, and production environments	510,303 €	4
8.5 Secure authentication	490,367 €	9
5.25 Assessment and decision on information security events	375,840 €	6

The most expensive failure relates to "Technical data integrity inconsistencies in systems leading to the confidentiality breach". Although this failure was not mapped to any specific ISO 27001 control, it can further be traced to controls that specify how information systems shall be developed and controls relating to "8.32 Change management", "5.12 Classification of information" and "8.29 Security testing in development and acceptance".

Further expensive failures result from inadequate "8.2 Privileged access rights". To prevent such incidents, the designation and use of privileged access rights should be restricted to ensure that only authorized users and service components are provided with privileged access [15]. More expensive failures resulted from the inadequacy of "8.5 Secure authentication", highlighting that a feasible authentication technique should be chosen to confirm the claimed identity of a user, software, messages, and other entities [15].

Expensive failures were also caused by the lack of control in "8.31 Separation of development, test, and production environments". In the absence of proper measures and procedures, developers and testers having access to production systems can introduce significant risks [15].

Expensive failures were caused by inadequacies in "8.7 Protection against malware", which should be based on malware detection, repair tools, and change management controls [15]. Many penalties were also caused by inadequacy in handling "5.24 Information security incident management planning and preparation", and further lack of implementation of control in "5.25 Assessment and decision on information security events".

C. Information security failure correlations

Table 4 presents the top three ISO/IEC 27001:2022 controls which have a positive correlation.

TABLE IV. TOP THREE POSITIVE FAILURE CORRELATIONS CORRESPONDING TO ISO/IEC 27001:2022 CONTROLS

Control 1	Control 2	Correlation	P-value
7.6 Working in secure areas	5.13 Labeling of information	1.00	***
5.26 Response to information security incidents	5.25 Assessment and decision on information security events	0.65	***
6.3 Information security awareness, education and training	5.10 Acceptable use of information and other associated assets	0.52	***
*$p < .05$, ** $p < .01$, *** $p < .001$			

The controls "7.6 Working in secure areas" and "5.13 Labeling of information" have a very strong correlation. In the analyzed cases, there were many data confidentiality breaches, where employees had not handled information within the organizations' physical premises in a secure way. Often, paper documents or other physical media containing sensitive personal data were carried outside of secure areas and were later found in waste bins by complete outsiders.

This observation can also be seen in the correlation of controls "6.3 Information security awareness, education and training" and "5.10 Acceptable use of information and other associated assets". Therefore, the organization should ensure that employees are made aware of how information should be handled, especially when it comes to PII [17].

Controls "5.25 Assessment and decision on information security events" and "5.26 Response to information security incidents" are naturally correlated together. If incidents are not reported, further investigated, and fixed, then incidents remain unaddressed, which consequently causes data breaches to become larger and more severe.

V. DISCUSSION

As the regulatory requirements to comply with information security are becoming more demanding, intelligence is needed to support the decision-making to select the most effective controls to manage risks and threats. GDPR penalty cases are a fruitful and transparent ground to explore information security failures, their impacts, and respective solutions based on control frameworks.

This study presented a novel statistical model to analyze the root causes of information security in GDPR penalty case documents and match those root causes with ISO/IEC 27001:2022 annex A controls. Our work bridged the gap between regulation and information security by providing previously unpublished information about information security failures and respective controls how to prevent those failures.

A. Conclusions

Inadequate access restrictions and management of privileged access rights were very typical causes of data breaches. Deficiencies in information security awareness, education and training led to several contrasting issues, as staff members did not know what was expected of them. The lack of applying a proper information classification scheme was a cause of many different shortcomings because, without risk assessments, further risk-based controls such as proper cryptographic techniques, adequate logging, relevant measures against malware, or adequate change management and system security testing could not be implemented. Technical data quality inconsistencies in systems leading to confidentiality breaches were the cause of the biggest penalty imposed by the supervisory authorities.

The top correlation was between inadequate data-labeling schemes and employees' mishandling of sensitive information. Many data confidentiality breaches were caused by careless staff members carrying documents containing sensitive personal data outside the facilities of an organization, which were later discovered in waste bins by outsiders. Improper control in information security incident management led to data breaches being unaddressed, which furthermore caused failures to become more severe and larger, and therefore the incident management controls were naturally correlated.

B. Limitations

Our study is subject to three noteworthy limitations. Firstly, the quality of the GDPR penalty case reports authored by various supervisory authorities across EU member states may differ. Specifically, the 81 penalty case reports analyzed may not adhere to a uniform structure, and their precision and length may vary. Secondly, the data source of our study, the GDPR Enforcement Tracker, may not be entirely up-to-date. It is conceivable that additional GDPR penalty cases, beyond the 81 analyzed, were issued in the year 2020, but not yet included in the database at the time this study was conducted.

Thirdly, the penalty calculations of our study cannot be considered definitive. While we have analyzed 81 GDPR penalty cases, all of which can be classified under the penalty type "insufficient technical and organizational measures to ensure information security", 25 of these cases also referenced other GDPR articles, beyond the scope of information security requirements. It is important to note that supervisory authorities issue GDPR penalties holistically and do not differentiate penalty amounts to address a specific article when levying a GDPR penalty against an organization.

C. *Further directions*

From a practical perspective, organizations and auditors implementing ISO/IEC 27001:2022 may use our results to apply and verify controls based on their impact and interdependence. We encourage further research which would analyze GDPR penalty cases with the statistical methods we applied in our study with the ISO/IEC 27001, as well as with other similar standardization frameworks.

From a broader perspective, researchers and information security practitioners at other institutions are encouraged to use this study as a motivation to popularize the assessed and ranked information security controls in order to effectively manage the complex and challenging information security risks in organizations.

REFERENCES

[1] M. Gerber and R. von Solms, "Information security requirements – interpreting the legal aspects," Computers and Security, vol. 27, pp. 124–135, 2008

[2] M.T. Tayyaba Tariq, S. Ali, M.T. Safraz, M.S. De-La-Hoz-Franco, E. Butt, S.A. Starcangelo, D.V. Rad and V. Rad, "Combination of AHP and TOPSIS methods for the ranking of information security controls to overcome its obstructions under fuzzy environment," Journal of Intelligent & Fuzzy Systems, vol. 38, pp. 6075–6088, 2020

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[4] J. Ruohonen and K. Hjerppe, "The GDPR enforcement fines at a glance," Information Systems, vol. 106, p. 101876, 2022

[5] B. von Solms, "Information security – the fourth wave," Computers and Security, vol. 25, pp. 165–168, 2006

[6] A. Vaibhav, "Information security governance metrics: a survey and taxonomy", Information Security Journal: A Global Perspective, vol. 31, pp. 466–478, 2022

[7] M. Siponen and R. Willison, "Information security management standards: problems and solutions," Information & Management, vol. 46, pp. 267–270, 2009

[8] A. Calder and L. Gerard, ISO 27001 / ISO 27002 a Pocket Guide, 2nd ed., Cambridgeshire: IT Governance Ltd, 2013, pp. 12–14

[9] V. Diamantopoulou, A. Tsohou and M. Karyda, "From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls," Information and Computer Security, vol. 28, 645–662, 2020

[10] M.T. Dlamini and J.H.P. Eloff and M.M. Eloff, "Information security: the moving target," Computers & Security, vol. 28, pp. 189–198, 2019

[11] C. Garrison and C. Hamilton, "A comparative analysis of the EU GDPR to the US's breach notifications," Information & Communications Technology Law, vol. 28, pp. 99–114, 2019

[12] J. Wolff and N. Atallah, "Early GDPR penalties: analysis of implementation and fines through May 2020", Journal of Information Policy, vol. 11, pp. 63–103,2021

[13] S. Akhlaghpour, F. Hassandoust, F. Fatehi, A. Burton-Jones, and A. Hynd, "Learning from enforcement cases to manage GDPR risks", MIS Quarterly Executive, vol. 20, pp. 199–218, 2021

[14] W. Presthus and K.F. Sønslien, "An analysis of violations and sanctions following the GDPR," International Journal of Information Systems and Project Management, vol. pp. 38–53, 2021

[15] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

[16] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

[17] ISO/IEC 27701:2019 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

[18] N.A. Chandra, R. Kalamullah, A.A.P. Ratna and T.S. Gunawan, "Information security risk assessment using situational awareness frameworks and application tools", Risks, vol. 10, pp. 165, 2022

[19] V. Monev, "Organisational information security maturity assessment based on ISO 27001 and ISO 27002", Proceedings of the 2020 IEEE International Conference on Information Technologies, 1-5, 2020

[20] B. Shojaie, H. Federrath and I. Saberi, "Evaluating the effectiveness of ISO 27001: 2013 based on annex A," Proceedings - 9th International Conference on Availability, Reliability and Security, 259-264, 2014

[21] H. Khajouei, M. Kazemi and S.H. Moosavirad, "Ranking information security controls by using fuzzy analytic hierarchy process," Information Systems and eBusiness Management, vol. 15, pp. 1–19, 2017

[22] M.I. Lopes, T. Guarda, and P. Oliveira, "Implementation of ISO 27001 standards as GDPR compliance facilitator", Journal of Information Systems Engineering and Management, vol. 4, 2019

[23] GDPR Enforcement Tracker, available at: https://www.enforcementtracker.com (accessed April-December 2021)

[24] J.J. Rooney, N. Lee and H. Vanden, "Root cause analysis for beginners," Quality Progress, vol. 37, pp. 45–53, 2004

[25] D. York, K. Jin, Q. Song, and H. Li, "Practical root cause analysis using cause mapping", Lecture Notes in Engineering and Computer Science, vol. 2, pp. 985–989, 2014

[26] Suorsa, M. and P. Helo, Information security failures identified and measured – ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis, Information Security Journal: A Global Perspective